S04P0878W000

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－169912
（Ｐ２００２－１６９９１２Ａ）
(43)公開日　平成14年６月14日(2002.6.14)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
G06F 17/60	142	G06F 17/60	142	5C064
	ZEC		ZEC	5J104
	302		302	E
	332		332	
G09C 1/00	660	G09C 1/00	660	B

審査請求　未請求　請求項の数14　ＯＬ　（全22頁）　最終頁に続く

(21)出願番号　特願2000－365576(Ｐ2000－365576)

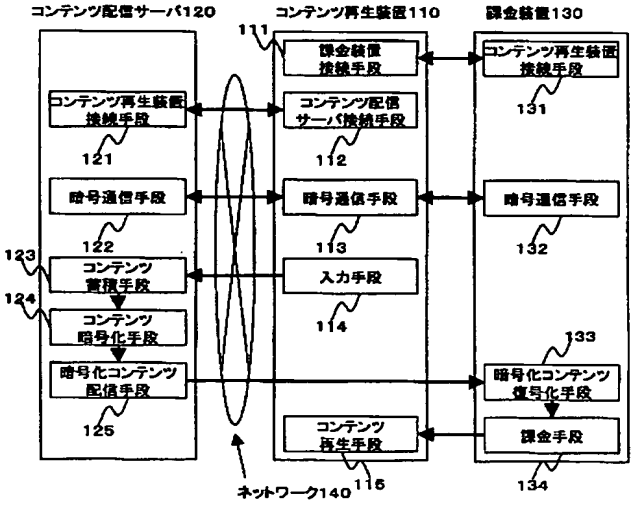
(22)出願日　平成12年11月30日(2000.11.30)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　丸山　純一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　兼平　晃
東京都小平市上水本町５丁目20番１号　株式会社日立製作所半導体グループ内
(74)代理人　100096954
弁理士　矢島　保夫

最終頁に続く

(54)【発明の名称】暗号復号化装置、課金装置、およびコンテンツ配信システム

(57)【要約】
【課題】コンテンツ配信システムにおいて、有償コンテンツの著作権を保護し、コンテンツの使用に際しては従量制で課金する。
【解決手段】コンテンツ配信サーバ１２０はコンテンツを暗号化して配信し、コンテンツ再生装置１１０は該暗号化コンテンツを復号化するために課金装置１３０を利用する。課金装置１３０は、該復号処理の使用を制限するバリュー値のカウンタを有し、該カウンタは復号化処理を行うとコンテンツの属性に応じて従量制で増減される。ユーザは対価を支払うことで、バリュー値を課金装置１３０に補充することができる。



【特許請求の範囲】

【請求項１】入力された暗号情報を復号化して出力する暗号復号化処理を行う手段を有する暗号復号化装置であって、

前記暗号復号化処理の実行を制御する制御情報を格納し、不正アクセスに対して耐性のある記憶手段と、

前記暗号復号化処理で処理した情報の量および該情報に定められた属性に応じて、前記記憶手段に格納された制御情報を更新する手段と、

前記制御情報に基づいて許可される場合に限り、前記暗号復号化処理の実行を許可する手段とを備えたことを特徴とする暗号復号化装置。

【請求項２】請求項１に記載の暗号復号化装置において、

情報を入力および出力する通信相手をそれぞれ認証する認証手段と、

前記通信相手と通信する際、前記認証手段によりそれぞれの通信相手が適当な通信相手として認証された場合に限り、情報の入力および出力を行い、さらに該入出力はそれぞれ暗号化して行う暗号通信手段とをさらに備えたことを特徴とする暗号復号化装置。

【請求項３】請求項１または２に記載の暗号復号化装置において、

前記暗号復号化処理を施すべき入力情報が複数の情報構成要素に分割された情報であり、該分割された各情報構成要素ごとに属性情報を有し、前記暗号復号化処理を情報構成要素に施したとき、その情報構成要素の属性情報に基づいて前記制御情報を更新することを特徴とする暗号復号化装置。

【請求項４】請求項１から３の何れか１つに記載の暗号復号化装置において、

前記制御情報は、前記暗号復号化処理を施した情報の対価を表す指標を含むことを特徴とする暗号復号化装置。

【請求項５】取得した情報の対価に応じて該情報の取得者に課金を行なう課金装置であって、

暗号化された入力情報を復号化して出力する暗号復号化処理を行う手段と、

取得する情報の対価の支払いのための価値を表すバリュー値を格納する記憶手段と、

前記暗号復号化処理で復号化処理して取得した情報の量および該情報の属性に応じて、前記記憶手段に格納されたバリュー値から、取得した情報の対価に相当する値を減少させる手段と、

前記バリュー値が所定値以上である場合に限り、前記暗号復号化処理の実行を許可する手段とを備えたことを特徴とする課金装置。

【請求項６】任意のコンテンツを配信し、該コンテンツの取得に対して課金を行うコンテンツ配信システムであって、

コンテンツを蓄積して配信するためのコンテンツ配信サーバと、前記コンテンツを取得し出力するためのコンテンツ再生装置と、前記コンテンツの取得に際して課金を行うための課金装置とを備え、

前記コンテンツ配信サーバは、

前記コンテンツ再生装置から送信されるコンテンツ送信要求を受信する手段と、

前記コンテンツ再生装置が発行するコンテンツ再生装置鍵を取得する手段と、

前記課金装置が発行する課金装置鍵を取得する手段と、

前記コンテンツ送信要求で要求されたコンテンツを前記コンテンツ再生装置鍵で暗号化し、さらに該暗号化したコンテンツを前記課金装置鍵で暗号化し、２重暗号化コンテンツとして出力する手段とを備え、

前記コンテンツ再生装置は、

ユーザから指示されたコンテンツの送信要求を前記コンテンツ配信サーバに送信する手段と、

コンテンツ再生装置鍵を発行する手段と、

前記課金装置から出力される前記コンテンツ再生装置鍵で暗号化されたコンテンツデータを取得する手段と、

前記コンテンツ再生装置鍵で暗号化されたコンテンツデータを前記コンテンツ再生装置鍵を用いて復号化し、平文のコンテンツを取得する手段とを備え、

前記課金装置は、

課金装置鍵を発行する手段と、

前記コンテンツ配信サーバから出力される２重暗号化コンテンツを取得する手段と、

該２重暗号化コンテンツを課金装置鍵を用いて復号化し、前記コンテンツ再生装置鍵で暗号化されたコンテンツデータを取得する手段と、

前記コンテンツ再生装置鍵で暗号化されたコンテンツデータを前記コンテンツ再生装置に送る手段とを備えていることを特徴とするコンテンツ配信システム。

【請求項７】請求項６に記載のコンテンツ配信システムにおいて、

前記コンテンツ配信サーバは、少なくとも１つ以上のコンテンツ再生装置に、少なくとも１つ以上のコンテンツを並行して同時に配信する手段を有し、

前記コンテンツ再生装置は、少なくとも１つ以上のコンテンツ配信サーバから、少なくとも１つ以上のコンテンツを並行して同時に取得する手段と、少なくとも１つ以上のコンテンツを並行して同時に再生する手段と、前記取得手段と再生手段を並行して同時に実行することが可能な手段とを有することを特徴とするコンテンツ配信システム。

【請求項８】請求項６または７に記載のコンテンツ配信システムにおいて、

前記課金装置は、

復号化する情報の対価の支払いのための価値を表すバリュー値を格納する記憶手段と、

復号化処理して取得した情報の量および該情報の属性に

応じて、前記記憶手段に格納されたバリュー値から、取得した情報の対価に相当する値を減少させる手段と、
前記バリュー値が所定値以上である場合に限り、前記暗号復号化処理の実行を許可する手段とをさらに備えたことを特徴とするコンテンツ配信システム。
【請求項９】請求項７または８に記載のコンテンツ配信システムにおいて、
配信されるコンテンツが複数の情報構成要素に分割された情報であり、該分割された各情報構成要素ごとに属性情報を有し、
前記課金装置は、復号化処理を情報構成要素に施したとき、復号化処理して取得した情報構成要素の情報量および該情報構成要素の属性に応じて、前記記憶手段に格納されたバリュー値から、取得した情報の対価に相当する値を減少させることを特徴とするコンテンツ配信システム。
【請求項１０】請求項７から９の何れか１つに記載のコンテンツ配信システムにおいて、
前記課金装置の記憶手段に格納されたバリュー値を増加させる手段を、さらに備えたことを特徴とするコンテンツ配信システム。
【請求項１１】請求項７から１０の何れか１つに記載のコンテンツ配信システムにおいて、
前記コンテンツ配信サーバは、前記コンテンツ再生装置の位置情報を取得する手段を備え、コンテンツの配信に際しては前記コンテンツ再生装置の位置に応じたコンテンツを配信することを特徴とするコンテンツ配信システム。
【請求項１２】請求項７から１１の何れか１つに記載のコンテンツ配信システムにおいて、
前記コンテンツ配信サーバが配信するコンテンツは、前記バリュー値を増加させるものを含み、
前記課金装置は、該バリュー値を増加させるコンテンツを復号化処理したとき、前記記憶手段内のバリュー値を増加させることを特徴とするコンテンツ配信システム。
【請求項１３】請求項７から１２の何れか１つに記載のコンテンツ配信システムにおいて、
前記バリューを減少させるコンテンツおよび前記バリュー値を増加させるコンテンツを配信するコーディネータを有し、前記コーディネータは、前記コンテンツ配信サーバを有し、コンテンツホルダから前記コンテンツの供給を受け、コンテンツの配信と代金の徴収を代行し、その対価にコンテンツホルダから手数料を受け取り、広告クライアントから広告コンテンツの供給を受け、広告コンテンツの配信を代行し、その対価に広告クライアントから広告料を受け取ることを特徴とするコンテンツ配信システム。
【請求項１４】コンテンツを蓄積して配信するためのコンテンツ配信サーバと、前記コンテンツを取得し出力するためのコンテンツ再生装置と、前記コンテンツの取得

に際して課金を行うための課金装置とを備えたコンテンツ配信システムにおけるコンテンツ配信方法であって、
前記コンテンツ配信サーバから暗号化されたコンテンツを取得し、該暗号化されたコンテンツを前記課金装置で復号化して、平文のコンテンツを取得するステップと、
前記課金装置により復号化を実行したとき、前記課金装置内に保持されている対価の支払いのための価値を表すバリュー値を更新するステップとを備えるとともに、
前記コンテンツは、前記課金装置で復号化されたとき前記バリュー値を減少させるコンテンツ、および前記課金装置で復号化されたときまたは平文のままで前記バリュー値を増加させるコンテンツを含むことを特徴とするコンテンツ配信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、サーバに蓄積されたオーディオ、ビデオ、あるいはテキストなどのコンテンツデータを、ユーザの所持するコンテンツ再生装置に対して適宜配信する技術に関し、特に、コンテンツの著作権保護および有償コンテンツへの課金を可能にする課金装置、並びに前記課金装置を用いたコンテンツ配信システムに関する。
【０００２】
【従来の技術】近年、オーディオやビデオなどのコンテンツデータを、インターネットなどのネットワークを介して配信しようとする試みがなされている。これはコンテンツを蓄積したコンテンツ配信サーバを用意し、ユーザはＰＣなどの端末からネットワークを介してコンテンツ配信サーバにアクセスし、コンテンツ配信サーバに蓄積されたコンテンツの中から目的とするコンテンツを取得し、クレジットカードなどの決済手段で対価を支払うシステムであり、例えば特開平１１－９６２３７号に記載のようなシステムが提案されている。該システムでは、コンテンツ配信サーバが各ユーザ毎のコンテンツ取得履歴のデータベースを有し、コンテンツデータの配信に伴って生じた課金を管理し、月単位などで区切って一括してクレジットカードによる決済を行う手法をとっている。また該システムでは、いわゆるストリーミング形式のコンテンツ配信にも対応しており、コンテンツデータを小単位に分割し、配信サーバが小単位毎に逐一データの配信を管理し、課金を施すことで従量制課金を実現している。
【０００３】
【発明が解決しようとする課題】前記のようなコンテンツ配信システムで扱われるコンテンツデータはデジタル化されており、複製が容易であるため、正当な権利を有する装置以外では使用できないようにする機能を設けたり、ネットワークを介して行われるデータの送受においても第３者の盗聴を防ぐ工夫を設けたりするなど、コンテンツの著作権を保護することが重要である。

【０００４】また有償のコンテンツデータを配信するシステムにおいては、コンテンツの代金の徴収手段が問題となる。例えばコンテンツを取得した後、料金を一括して支払うシステムでは、コンテンツ取得が確実に終了したことを確認する手段が必要となり、コンテンツの取得がなんらかの事由で中断された場合などは、再接続などの手順が必要になり、処理が複雑になってしまう。また、いわゆるストリーミング配信形式のコンテンツに関しては、コンテンツストリーム１本の取得につきいくら、といった形式での課金方法もあるが、この場合、視聴を途中で終了しても、課金は全て行われてしまうという問題がある。

【０００５】これらの問題を解決するための方法のひとつに、例えば上述した特開平１１－９６２３７号において提案されているような、コンテンツを使用した量に応じて課金する従量制課金方式があるが、該システムのように課金状況をコンテンツ配信サーバの所持する履歴情報によって管理し、クレジットカードを使用して課金処理を行う決済手段では、システム利用に対してはあらかじめユーザがサーバに登録する必要があること、またコンテンツのやり取りと決済との間に時差が生じ、ユーザが課金された金額をリアルタイムで知ることができないこと、などの不都合が生じる。

【０００６】本発明は、前記事情に鑑みてなされたものであり、その目的は、コンテンツの著作権を保護する機能と、従量制によるコンテンツの課金機能を有するコンテンツ配信システムを提供することにある。

【０００７】

【課題を解決するための手段】上記目的を達成するため、本発明は、入力された暗号情報を復号化して出力する暗号復号化処理を行う手段を有する暗号復号化装置であって、前記暗号復号化処理の実行を制御する制御情報を格納し、不正アクセスに対して耐性のある記憶手段と、前記暗号復号化処理で処理した情報の量および該情報に定められた属性に応じて、前記記憶手段に格納された制御情報を更新する手段と、前記制御情報に基づいて許可される場合に限り、前記暗号復号化処理の実行を許可する手段とを備えたことを特徴とする。

【０００８】また本発明は、上記暗号復号化装置において、情報を入力および出力する通信相手をそれぞれ認証する認証手段と、前記通信相手と通信する際、前記認証手段によりそれぞれの通信相手が適当な通信相手として認証された場合に限り、情報の入力および出力を行い、さらに該入出力はそれぞれ暗号化して行う暗号通信手段とをさらに備えたことを特徴とする。これにより、正当な権利を有する装置以外でコンテンツが不正に利用されることを防ぐ。

【０００９】また本発明は、上記暗号復号化装置において、前記暗号復号化処理を施すべき入力情報が複数の情報構成要素に分割された情報であり、該分割された各情報構成要素ごとに属性情報を有し、前記暗号復号化処理を情報構成要素に施したとき、その情報構成要素の属性情報に基づいて前記制御情報を更新することを特徴とする。

【００１０】また本発明は、取得した情報の対価に応じて該情報の取得者に課金を行なう課金装置であって、暗号化された入力情報を復号化して出力する暗号復号化処理を行う手段と、取得する情報の対価の支払いのための価値を表すバリュー値を格納する記憶手段と、前記暗号復号化処理で復号化処理して取得した情報の量および該情報の属性に応じて、前記記憶手段に格納されたバリュー値から、取得した情報の対価に相当する値を減少させる手段と、前記バリュー値が所定値以上である場合に限り、前記暗号復号化処理の実行を許可する手段とを備えたことを特徴とする。

【００１１】また本発明は、任意のコンテンツを配信し、該コンテンツの取得に対して課金を行うコンテンツ配信システムであって、コンテンツを蓄積して配信するためのコンテンツ配信サーバと、前記コンテンツを取得し出力するためのコンテンツ再生装置と、前記コンテンツの取得に際して課金を行うための課金装置とを備え、前記コンテンツ配信サーバは、前記コンテンツ再生装置から送信されるコンテンツ送信要求を受信する手段と、前記コンテンツ再生装置が発行するコンテンツ再生装置鍵を取得する手段と、前記課金装置が発行する課金装置鍵を取得する手段と、前記コンテンツ送信要求で要求されたコンテンツを前記コンテンツ再生装置鍵で暗号化し、さらに該暗号化したコンテンツを前記課金装置鍵で暗号化し、２重暗号化コンテンツとして出力する手段とを備え、前記コンテンツ再生装置は、ユーザから指示されたコンテンツの送信要求を前記コンテンツ配信サーバに送信する手段と、コンテンツ再生装置鍵を発行する手段と、前記課金装置から出力される前記コンテンツ再生装置鍵で暗号化されたコンテンツデータを取得する手段と、前記コンテンツ再生装置鍵で暗号化されたコンテンツデータを前記コンテンツ再生装置鍵を用いて復号化し、平文のコンテンツを取得する手段とを備え、前記課金装置は、課金装置鍵を発行する手段と、前記コンテンツ配信サーバから出力される２重暗号化コンテンツを取得する手段と、該２重暗号化コンテンツを課金装置鍵を用いて復号化し、前記コンテンツ再生装置鍵で暗号化されたコンテンツデータを取得する手段と、前記コンテンツ再生装置鍵で暗号化されたコンテンツデータを前記コンテンツ再生装置に送る手段とを備えていることを特徴とする。

【００１２】また本発明は、上記コンテンツ配信システムにおいて、前記コンテンツ配信サーバは、少なくとも１つ以上のコンテンツ再生装置に、少なくとも１つ以上のコンテンツを並行して同時に配信する手段を有し、前記コンテンツ再生装置は、少なくとも１つ以上のコンテ

ンツ配信サーバから、少なくとも１つ以上のコンテンツを並行して同時に取得する手段と、少なくとも１つ以上のコンテンツを並行して同時に再生する手段と、前記取得手段と再生手段を並行して同時に実行することが可能な手段とを有することを特徴とする。

【００１３】また本発明は、上記コンテンツ配信システムにおいて、前記課金装置は、復号化する情報の対価の支払いのための価値を表すバリュー値を格納する記憶手段と、復号化処理して取得した情報の量および該情報の属性に応じて、前記記憶手段に格納されたバリュー値から、取得した情報の対価に相当する値を減少させる手段と、前記バリュー値が所定値以上である場合に限り、前記暗号復号化処理の実行を許可する手段とをさらに備えたことを特徴とする。

【００１４】また本発明は、上記コンテンツ配信システムにおいて、配信されるコンテンツが複数の情報構成要素に分割された情報であり、該分割された各情報構成要素ごとに属性情報を有し、前記課金装置は、復号化処理を情報構成要素に施したとき、復号化処理して取得した情報構成要素の情報量および該情報構成要素の属性に応じて、前記記憶手段に格納されたバリュー値から、取得した情報の対価に相当する値を減少させることを特徴とする。

【００１５】また本発明は、上記コンテンツ配信システムにおいて、前記課金装置の記憶手段に格納されたバリュー値を増加させる手段を、さらに備えたことを特徴とする。

【００１６】また本発明は、上記コンテンツ配信システムにおいて、前記コンテンツ配信サーバは、前記コンテンツ再生装置の位置情報を取得する手段を備え、コンテンツの配信に際しては前記コンテンツ再生装置の位置に応じたコンテンツを配信することを特徴とする。

【００１７】また本発明は、上記コンテンツ配信システムにおいて、前記コンテンツ配信サーバが配信するコンテンツは、前記バリュー値を増加させるものを含み、前記課金装置は、該バリュー値を増加させるコンテンツを復号化処理したとき、前記記憶手段内のバリュー値を増加させることを特徴とする。

【００１８】また本発明は、上記コンテンツ配信システムにおいて、前記バリューを減少させるコンテンツおよび前記バリュー値を増加させるコンテンツを配信するコーディネータを有し、前記コーディネータは、前記コンテンツ配信サーバを有し、コンテンツホルダから前記コンテンツの供給を受け、コンテンツの配信と代金の徴収を代行し、その対価にコンテンツホルダから手数料を受け取り、広告クライアントから広告コンテンツの供給を受け、広告コンテンツの配信を代行し、その対価に広告クライアントから広告料を受け取ることを特徴とする。

【００１９】さらに本発明は、コンテンツを蓄積して配信するためのコンテンツ配信サーバと、前記コンテンツ

を取得し出力するためのコンテンツ再生装置と、前記コンテンツの取得に際して課金を行うための課金装置とを備えたコンテンツ配信システムにおけるコンテンツ配信方法であって、前記コンテンツ配信サーバから暗号化されたコンテンツを取得し、該暗号化されたコンテンツを前記課金装置で復号化して、平文のコンテンツを取得するステップと、前記課金装置により復号化を実行したとき、前記課金装置内に保持されている対価の支払いのための価値を表すバリュー値を更新するステップとを備えるとともに、前記コンテンツは、前記課金装置で復号化されたとき前記バリュー値を減少させるコンテンツ、および前記課金装置で復号化されたときまたは平文のままで前記バリュー値を増加させるコンテンツを含むことを特徴とする。

【００２０】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【００２１】図１は、本発明の一実施形態が適用されたコンテンツ配信システムの概略構成を示す図である。

【００２２】図１において、コンテンツ再生装置１１０は、オーディオ、ビデオ、およびテキストなどのコンテンツの再生を行う機能と、コンテンツ配信サーバ１２０にアクセスしてコンテンツの取得を行う機能を備えた装置であり、課金装置接続手段１１１、コンテンツ配信サーバ接続手段１１２、暗号通信手段１１３、入力手段１１４、およびコンテンツ再生手段１１５を有する。コンテンツ再生装置１１０は、例えば、携帯型ビューア、セットトップボックス、あるいはＰＣなどの形態をとることができる。

【００２３】コンテンツ配信サーバ１２０は、コンテンツの蓄積と配信を行う装置であり、コンテンツ再生装置接続手段１２１、暗号通信手段１２２、コンテンツ蓄積手段１２３、コンテンツ暗号化手段１２４、および暗号化コンテンツ配信手段１２５を有する。コンテンツ配信サーバ１２０は、コンテンツ再生装置１１０からのコンテンツ取得要求を受けて、適宜コンテンツを配信する。

【００２４】課金装置１３０は、コンテンツ再生装置１１０が有償コンテンツの取得あるいは再生などの処理を行う際に、課金を行う装置であり、コンテンツ再生装置接続手段１３１、暗号通信手段１３２、暗号化コンテンツ復号化手段１３３、および課金手段１３４を有する。課金装置１３０は、コンテンツ再生装置１１０に内蔵することにしてもよいし、コンテンツ再生装置１１０に着脱自在な形態をとってもよい。また課金装置１３０は、半導体チップのような形態として、ＩＣカードやメモリーカードなどの記録装置などに付加したり、あるいはハードディスクなどの磁気記録媒体に付加して、該課金機能を提供することにしてもよい。また、bluetoothのような無線通信機能をもたせ、非接触の通信によって上記機能をコンテンツ再生装置１１０に提供する形態として

もよい。

【００２５】ネットワーク１４０は、コンテンツ再生装置１１０とコンテンツ配信サーバ１２０の通信経路であって、例えばインターネット、オンラインシステム、あるいは無線通信網などである。コンテンツ配信サーバ１２０からコンテンツ再生装置１１０への情報伝達経路と、コンテンツ再生装置１１０からコンテンツ配信サーバ１２０への情報伝達経路とを異なるものにしてもよい。例えば前者には衛星放送やケーブルテレビ網などを利用し、後者には電話回線や無線通信などを利用することもできる。

【００２６】前記の装置構成によって実現される著作権保護機能および従量制課金機能を備えたコンテンツ配信システムの処理フローの概略は例えば次のようになる。

【００２７】課金装置接続手段１１１とコンテンツ再生装置接続手段１３１を利用して、コンテンツ再生装置１１０と課金装置１３０とが接続される。続いて、コンテンツ再生装置接続手段１２１とコンテンツ配信サーバ接続手段１１２を利用して、コンテンツ配信サーバ１２０とコンテンツ再生装置１１０とが接続される。

【００２８】前記の手段によって装置間の通信が確保された後、入力手段１１４によってユーザからのコンテンツの取得指示を受けたコンテンツ再生装置１１０は、まずコンテンツ配信サーバ１２０にコンテンツの配信要求を送る。それを受けたコンテンツ配信サーバ１２０は、コンテンツ蓄積手段１２３に蓄積されたコンテンツ群の中の該当するコンテンツを、コンテンツ暗号化手段１２４を用いて暗号化し、次に暗号化コンテンツ配信手段１２５を利用してコンテンツ再生装置１１０に送信する。ここで暗号化されたコンテンツデータはそのままでは再生することができないため、コンテンツ再生装置１１０は課金装置１３０の暗号化コンテンツ復号化手段１３３を用いて該暗号化コンテンツデータを復号し、同時に課金装置１３０は課金手段１３４によってコンテンツ使用に対する課金を行う。最後にコンテンツ再生装置１１０は、復号化されたコンテンツデータをコンテンツ再生手段１１５を用いて再生する。

【００２９】前記処理の過程で行われる装置間の通信の安全性を確保するために、暗号通信手段１１３、１２２、１３２が利用される。ここで言う暗号通信手段とは、例えば通信相手を認証する手段と、情報を暗号化するための鍵を通信相手に発行する手段と、通信相手が該鍵を用いて暗号化した情報を復号化するための手段と、の組によって実現できる。

【００３０】次に、本コンテンツ配信システムを構成する各装置のうち、コンテンツ再生装置１１０および課金装置１３０について、さらに詳細に説明する。

【００３１】まずコンテンツ再生装置１１０について説明する。

【００３２】図２は、コンテンツ再生装置１１０の概略構成の一例を示す図である。ＣＰＵ２０１は、コンテンツ再生装置１１０の各部を統括的に制御する。メモリ２０２は、ＲＯＭおよびＲＡＭから構成される。ＲＯＭには、ＣＰＵ２０１が本コンテンツ再生装置１１０の各部を統括的に制御するためのプログラムが格納されている。ＲＡＭは、ＣＰＵ２０１のワークエリアとして機能する。

【００３３】通信装置２０４は、コンテンツ配信サーバ１２０にアクセスするのに用いられる。無線通信手段であってもよいし、有線通信手段であってもよい。またそれらの通信手段を複数備えていても良い。コンテンツ配信サーバ１２０以外に、他のコンテンツ再生装置１１０やＰＣなどの各種装置と通信する手段を有していても良い。

【００３４】入力装置２０３は、例えば各種ボタンやタッチパネルで構成され、ユーザからの再生指示やコンテンツデータの入手指示などを受け付ける。表示装置２０８は、例えば液晶パネルで構成され、コンテンツのリストを表示したり、ビデオ再生装置２０７で再生されたビデオコンテンツを表示したりする。オーディオ再生装置２０６は、暗号化されたコンテンツを復号し、オーディオ信号を得る。そして、オーディオ信号を本コンテンツ再生装置１１０に内蔵されたスピーカー（不図示）や外付けのヘッドフォンなどに出力する。ビデオ再生装置２０７は、暗号化されたコンテンツを復号し、ビデオ信号を得る。そして、ビデオ信号を本コンテンツ再生装置１１０に内蔵された表示装置２０８や、外付けのモニターなどに出力する。

【００３５】課金装置接続装置２０５は、課金装置１３０を接続し、課金装置１３０からデータを入手したり、課金装置１３０へデータを送ったりする。インターフェース２０９は、ＣＰＵ２０１やメモリ２０２と本コンテンツ再生装置１１０を構成する他装置との間のデータ送受を司る。

【００３６】次に、オーディオ再生装置２０６について説明する。

【００３７】図３は、オーディオ再生装置２０６の概略構成を示す図である。図示するように、オーディオ再生装置２０６は、暗復号化回路３０２と、デコーダ回路３０３と、インターフェース２０９を介して本コンテンツ再生装置１１０の各部とデータ送受を行うためのＩ／Ｏ回路３０１と、を有する。

【００３８】暗復号化回路３０２は、外部装置との相互認証機能を有し、また前記装置間でデータを暗号化して送受する機能を備える。暗復号化回路３０２は、例えばオーディオ再生装置鍵を発行する手段を有し、該オーディオ再生装置鍵で暗号化されたコンテンツを入力とし、該オーディオ再生装置鍵で復号して、デコーダ回路３０３へ出力する。デコーダ回路３０３は、暗復号化回路３０２から出力されたオーディオデータを、必要に応じて

伸張、再生して、オーディオ信号を得る。そして、オーディオ信号をスピーカーなどに出力する。ここで図に示すオーディオ再生装置２０６を構成する各部は、例えば１チップ上につくりこまれる。

【００３９】次に、ビデオ再生装置２０７について説明する。

【００４０】図４は、ビデオ再生装置２０７の概略構成を示す図である。図示するように、ビデオ再生装置２０７は、暗復号化回路４０２と、デコーダ回路４０３と、インターフェース２０９を介して本コンテンツ再生装置１１０の各部とデータ送受を行うためのＩ／Ｏ回路４０１と、を有する。

【００４１】暗復号化回路４０２は、外部装置との相互認証機能を有し、また前記装置間でデータを暗号化して送受する機能を備える。暗復号化回路４０２は、例えばビデオ再生装置鍵を発行する手段を有し、該ビデオ再生装置鍵で暗号化されたコンテンツを入力とし、該オーディオ再生装置鍵で復号して、デコーダ回路４０３へ出力する。デコーダ回路４０３は、暗復号化回路４０２から出力されたビデオデータを、必要に応じて伸張、再生して、ビデオ信号を得る。そして、ビデオ信号を表示装置やモニタなどに出力する。ここで図に示すビデオ再生装置２０７を構成する各部は、例えば１チップ上につくりこまれる。またビデオ表示装置にビデオ再生装置２０７を内蔵させてもよいし、オーディオ再生装置２０６とビデオ再生装置２０７とをあわせて１チップ上につくりこんでもよい。また、これらの再生装置は、ソフトウエアで実現してもよい。

【００４２】なお、以降の説明では、オーディオ再生装置鍵とビデオ再生装置鍵とを合わせてコンテンツ再生装置鍵として記述する。

【００４３】図５は、課金装置１３０の概略構成を示す図である。課金装置１３０は、暗復号化回路５０１、課金回路５０２、記憶回路５０５、および課金装置接続装置２０５とのインターフェースであるＩ／Ｏ回路５０４を有する。

【００４４】暗復号化回路５０１は、認証機能と暗復号化機能を有している。記憶回路５０５には暗復号化回路５０１の動作を制限するバリュー値カウンタ５０３が設けられている。バリュー値カウンタ５０３は、課金装置１３０が蓄積しているバリューの量を記憶するための手段を有する。バリューとは、コンテンツの価値を表す概念であり、例えば金銭を代替するものである。バリューの量の記憶手段は、例えば、バリューが増加するとカウンタが増加することにしてもよいし反対にカウンタが減少することにしてもよい。該バリュー値カウンタ５０３の値が所定の範囲にある場合に限り、暗復号化回路５０１は前記暗号復号化処理を行なうことができる。すなわち、ユーザが有料のコンテンツを取得する際にはこのバリュー値で対価を支払うので、バリュー値が所定値以上ないときは復号化処理を行なうことができないようにして、コンテンツの取得ができないように制限している。

【００４５】課金回路５０２は、暗復号化回路５０１によって処理された情報の量と属性によってバリュー値カウンタ５０３を変化させる機能を有している。ここで暗復号化回路５０１、課金回路５０２、および記憶回路５０５は、セキュリティを強化するため、いわゆるタンパ・レジスタント領域(TRM: Tamper Resistant Module)５０６に格納するのがよい。

【００４６】また、暗復号化回路５０１および課金回路５０２などは、例えば、前記機能を有するプログラムと、前記プログラムを格納するためのメモリと、前記プログラムを実行するためのＣＰＵとによって実現される構成にしてもよい。

【００４７】前記課金装置１３０を構成する各部は、例えば１チップ上につくりこまれるようにしてもよいし、あるいは、複数チップで構成されるようにしてもよい。複数チップで構成する場合は、課金装置１３０の外部からチップ間の信号を読み取られないような工夫を施すことが望ましい。

【００４８】次に、本コンテンツ配信システムにおいて各装置間で行われる通信の手順の一例について説明する。

【００４９】図６は、コンテンツの再生時に課金をするシステムの一構成例である。ここで、コンテンツ再生装置１１０および課金装置１３０は、それぞれデータを暗号化するための鍵を発行する手段と、該鍵で暗号化されたデータを復号化するための手段を持つ。ここで該鍵は、各装置毎にユニークな鍵を予め各装置が有していても良いし、乱数などによって毎回作成しても良い。ただし、該鍵は認証によって所有を許可された正当な装置以外には知られないようにする。

【００５０】コンテンツ再生装置１１０は、コンテンツ配信サーバ１２０に、コンテンツの配信要求と、コンテンツ再生装置鍵Kpを送信する（６０１）。次に、課金装置１３０が、コンテンツ配信サーバ１２０に課金装置鍵Kcを送信する（６０２）。それを受けて、コンテンツ配信サーバ１２０は、要求されたコンテンツDを、コンテンツ再生装置鍵Kpで暗号化し、さらに該暗号化コンテンツE(Kp,D)を課金装置鍵Kcで暗号化する。次にコンテンツ配信サーバ１２０は、該２重暗号化コンテンツE(Kc,E(Kp,D))を課金装置１３０に送信する（６０３）。ここで、２重暗号化コンテンツE(Kc,E(Kp,D))は、そのままではコンテンツ再生装置１１０で再生することはできないため、コンテンツを再生するには、課金装置１３０が必要になる。

【００５１】課金装置１３０は、受信した２重暗号化コンテンツE(Kc,E(Kp,D))を自身の保持する課金装置鍵Kcで復号し、その際の処理量に応じてバリュー値のカウンタVを変化させる（６０４）。続いて、復号化されたコ

ンテンツE(Kp,D)をコンテンツ再生装置１１０に送信する（６０５）。また、該課金装置１３０の保持するバリュー値Vが所定の範囲の値をとる場合、課金装置１３０は、２重暗号化コンテンツの復号を行うことができないようにする。そのため、ユーザは、コンテンツ再生のためにある程度のバリュー値の取得が必要になる。

【００５２】該暗号化コンテンツを受信したコンテンツ再生装置１１０は、自身の保持するコンテンツ再生装置鍵Kpで該暗号化コンテンツE(Kp,D)を復号し、復号化された平文のコンテンツDを再生する。ここで、コンテンツ再生装置１１０が受信した暗号化コンテンツE(Kp,D)は、該コンテンツ再生装置鍵Kpを持つコンテンツ再生装置１１０以外では復号化することができないため、不正コピーを防ぐことができる。

【００５３】以上の処理において、コンテンツ再生装置鍵Kpと課金装置鍵Kcは、それぞれの装置のもつ認証機能と暗号通信機能を利用して安全に送受される。

【００５４】図７に、以上に示したやり取りをフロー図で表す。まず、コンテンツ再生装置１１０が、コンテンツ配信サーバ１２０と課金装置１３０の双方に自身の認証を要求する（ステップ７０１～７０４）。認証が正常に行われた場合は、コンテンツ再生装置１１０が、コンテンツ配信サーバ１２０にコンテンツの送信要求と共に、コンテンツ再生装置鍵Kpを送信する（ステップ７０５）。つづいてコンテンツ配信サーバ１２０と課金装置１３０との間で相互に認証が行われる（ステップ７０５～７０９）。コンテンツ配信サーバ１２０が課金装置１３０に認証を要求し、認証が正常に行われた場合は、課金装置１３０がコンテンツ配信サーバ１２０に認証要求と課金装置鍵Kcを送信する（ステップ７０８）。それを受けてコンテンツ配信サーバ１２０は、要求されたコンテンツDをまずコンテンツ再生装置鍵Kpで暗号化し、さらに課金装置鍵Kcで暗号化して課金装置１３０に送信する（ステップ７１０）。それを受けて課金装置１３０は、課金装置鍵Kcで２重暗号化コンテンツE(Kc,E(Kp,D))を１回復号化し、該コンテンツE(Kp,D)をコンテンツ再生装置１１０に送信する（ステップ７１１）。最後にコンテンツ再生装置１１０が、受信した暗号化コンテンツE(Kp,D)をコンテンツ再生装置鍵Kpで復号化し、コンテンツDを再生する（ステップ７１２）。

【００５５】前記各手順において、認証などの処理が正常に行われなかった場合は、エラー処理（ステップ７１３）をして終了する。

【００５６】また図８は、図６および図７を用いて説明したコンテンツ配信システムにおける、装置間のデータ送受手順の一例を示したシーケンス図である。

【００５７】コンテンツ再生装置１１０は、コンテンツ配信サーバ１２０から認証を受けるため、コンテンツ再生装置１１０の公開鍵KPpとその公開鍵の証明書C(KPp)を含む認証要求をコンテンツ配信サーバ１２０に送信する（８０１）。

【００５８】これを受けて、コンテンツ配信サーバ１２０は、コンテンツ再生装置１１０の認証および公開鍵KPpの正当性の検証を行う（８０２）。次にセッション鍵Ks1を生成し（８０３）、これをKPpで暗号化してコンテンツ再生装置１１０に送信する（８０４）。

【００５９】これを受けたコンテンツ再生装置１１０は、暗号化されたKs1を秘密鍵Kpで復号化し、セッション鍵Ks1を得る。セッション鍵Ks1を確認した後（８０５）、コンテンツ再生装置１１０は、続いて課金装置１３０から認証を受けるため、コンテンツ再生装置１１０の公開鍵KPdとその公開鍵の証明書C(KPd)を含む認証要求を課金装置１３０に送信する（８０６）。

【００６０】これを受けて、課金装置１３０は、コンテンツ再生装置１１０の認証および公開鍵KPdの正当性の検証を行う（８０７）。次にセッション鍵Ks2を生成し（８０８）、これをKPdで暗号化してコンテンツ再生装置１１０に送信する（８０９）。

【００６１】これを受けたコンテンツ再生装置１１０は、暗号化されたKs2を秘密鍵Kpで復号化し、セッション鍵Ks2を得る。セッション鍵Ks2を確認した後（８１０）、コンテンツ再生装置１１０は、続いてセッション鍵Ks3を生成し（８１１）、セッション鍵Ks2およびKs3をセッション鍵Ks1で暗号化した情報を含むコンテンツ送信要求をコンテンツ配信サーバ１２０に送信する（８１２）。

【００６２】これを受けたコンテンツ配信サーバ１２０は、セッション鍵Ks1を用いて復号化し、Ks2およびKs3を得る。セッション鍵Ks2およびKs3を確認した後（８１３）、セッション鍵Ks4を生成し（８１４）、コンテンツ配信サーバ１２０は、続いて課金装置１３０に認証を受けるため、自身の認証データC(Server)を課金装置１３０に送信する（８１５）。ここで認証データC(Server)は、セッション鍵Ks4と共にセッション鍵Ks2を用いて暗号化されている。

【００６３】これを受けて、課金装置１３０は、セッション鍵Ks2を用いて認証データC(Server)およびセッション鍵Ks4を復号し、コンテンツ配信サーバ１２０の認証およびセッション鍵Ks4の確認を行う（８１６、８１７）。認証と確認が正常に行われた場合は、自身の認証データC(Charge)と課金装置鍵Kcをセッション鍵Ks4で暗号化してコンテンツ配信サーバ１２０に送信する（８１８）。

【００６４】これを受けて、コンテンツ配信サーバ１２０は、セッション鍵Ks4を用いて認証データC(Charge)および課金装置鍵Kcを復号し、課金装置１３０の認証および課金装置鍵Kcの確認を行う（８１９、８２０）。認証と確認が正常に行われた場合は、コンテンツデータDをセッション鍵Ks3で暗号化し、さらに課金装置鍵Kcで暗号化した２重暗号化コンテンツデータを課金装置１３０

に送信する（８２１）。

【００６５】これを受けて、課金装置１３０は、課金装置鍵Kcを用いて２重暗号化コンテンツデータを復号化し、セッション鍵Ks3によって暗号化されたコンテンツデータDを得る。そして該コンテンツデータの属性情報に基づいてバリュー値Vを変化させた後（８２２）、暗号化コンテンツデータをコンテンツ再生装置１１０に送信する（８２３）。

【００６６】これを受けて、コンテンツ再生装置１１０は、セッション鍵Ks3を用いて暗号化コンテンツデータを復号化し、コンテンツデータDを取得し、該コンテンツデータを再生する（８２４）。

【００６７】次に、図９に本実施形態が適用されたコンテンツ配信システムの一例を示す。課金装置１３０は、前述のように、暗号化コンテンツ復号手段と課金手段を有し、暗号化コンテンツの復号化処理を実行した場合、従量制で課金する機能を有する。該課金手段はバリュー値カウンタ５０３を有し、そのカウンタの値によって前記復号化処理の制限を行う。例えば、カウンタがある範囲の値をとる場合に限り、前記復号化処理を利用可能なようにする。もしくはカウンタの値によって記憶装置９０６の機能を変えるようにしてもよい。例えば、カウンタ値が一定値以上の場合は課金装置１３０の機能に加えて付加サービスを利用できるようにすることもできる。また課金装置１３０の記憶回路５０５に、コンテンツ取得の履歴情報などを保存する機能を設けることもできる。この履歴情報を利用し、例えば一度課金したコンテンツを再び利用する際には課金を行わないようにする、利用回数を重ねると割引を行うようにする、などの処理を行うこともできる。

【００６８】本コンテンツ配信システムにおいて、バリュー値とはコンテンツの価値を表す指標であり、コンテンツの価値に見合うようにコンテンツホルダ９０２やコーディネータ９０１などによって設定、発行され、コンテンツの属性情報としてコンテンツに付加される。コンテンツの配信に伴うコンテンツホルダ９０２とユーザとの間の代金の授受はバリューを介して行われる。ユーザは対価を支払ってバリューの発行を受ける。ユーザは予めバリュー値の補充された課金装置１３０を購入することもできるし、後からバリュー値のみを補充することもできる。

【００６９】さらに、図１０に示すように、バリュー値カウンタVの変化量は、コンテンツD全体に対して一括して設定されるだけでなく、コンテンツの構成要素（D1～D8）毎に設定することもできる。ここで言うコンテンツの構成要素には、例えば単位時間で区切られたコンテンツの小部分を充てることができ、この場合、コンテンツの各時刻毎の内容に応じてバリュー値の変化量α(Dx)を設定することとなる。また、データのビット数やシーン数などによってコンテンツを分割し、分割された各小部分を構成要素Dxとみなすこともできる。これにより、例えば映像のコンテンツをユーザに提供する場合に部分的に課金を設定でき、重要な場面や人気の高い場面については部分的に課金額を変えたりするなど、柔軟な従量制の課金を行うことができる。

【００７０】また、例えばバリュー値カウンタVによる暗号復号化処理の制限方法を、暗号復号化処理を行うとバリュー値が減少し、カウンタが一定値以上の場合に限り、暗号復号化処理を行うように設定した場合、D1、D2、D3、D4、D7に示すようなバリュー値を減算させる属性を付加したコンテンツは有償コンテンツとして扱い、D6、D8に示すようなバリュー値を増加させる属性を付加したコンテンツは、視聴したユーザに特典を与えるバリュー増加コンテンツとして扱うことができる。これにより、有償コンテンツを見るとバリュー値が減るが、広告などのコンテンツを見ればバリュー値が増加する、といったサービスも提供できる。

【００７１】また、ユーザは、課金装置のバリュー値を対価に支払うことで、コンテンツ配信以外の各種サービスを受けることができることにしても良い。例えばバリュー値の支払いの対価に他の物品を取得することができたりしても良い。

【００７２】コンテンツ再生装置１１０は、前記のように、オーディオ、ビデオ、あるいはテキストなどのコンテンツの再生を行う機能と、コンテンツ配信サーバ１２０にアクセスしてコンテンツの取得を行う機能を備えた装置である。この通信手段は、無線もしくは有線、あるいはその両方でも良い。また、コンテンツ再生装置１１０は、課金装置１３０の接続装置を内蔵し、コンテンツ配信サーバ１２０との間で行う通信を中継する手段を有する課金装置１３０をここに接続することで、有償コンテンツの取得および再生が可能となる。無償のコンテンツを再生する場合は、課金装置１３０の接続を必要としないことにすることもできる。コンテンツ再生装置１１０は、課金装置１３０内のバリュー値のカウンタを表示する機能を備えていても良い。

【００７３】上述した例では１つのコンテンツ配信サーバ１２０にアクセスする例で説明したが、該コンテンツ再生装置１１０および課金装置１３０は、複数のコンテンツ配信サーバ１２０にアクセスし、並行して同時に複数のコンテンツを取得することが可能としてもよい。また複数のコンテンツを並行して同時に再生する手段を有していてもよい。例えば、表示装置の表示領域を分割し、分割された画面それぞれに別のコンテンツを再生したり、別個のオーディオコンテンツとビデオコンテンツを同時に再生したりする。さらに、前記取得手段と再生手段を並行して同時に実行する手段を有していても良い。前記の並列処理を行う場合、課金装置１３０内のバリュー値カウンタの変化も各コンテンツ毎に同時に並行して行われることにする。

【００７４】コーディネータ９０１は、コンテンツを配信するためのコンテンツ配信サーバ１２０を有し、コンテンツの配信をコンテンツホルダ９０２に代わって代行する業者であり、コンテンツホルダ９０２からコンテンツの供給を受け、蓄積しておき、ユーザの所有する再生装置１１０からの要求に応じて適宜コンテンツを配信する。コーディネータ９０１は、ユーザからコンテンツ取得および配信サービスの利用の対価を徴収し、コンテンツホルダ９０２に支払う。その際、配信および代金徴収を代行する手数料をコンテンツホルダ９０２から受け取る。またコーディネータ９０１は、広告クライアント９０３からの委託をうけ、ユーザに広告コンテンツを配信し、配信した広告コンテンツの量に応じてその対価（広告代理店としての報酬）を受け取る。広告コンテンツの配信に際しては、個々の広告コンテンツに設定されている配布対象地域情報と、配信対象のユーザの位置情報とを合わせて利用し、配信する広告コンテンツを決定するとよい。こうして地域に密接した広告コンテンツを配信することで、広告効果を高めることができる。なお、コーディネータ９０１は、ユーザからの要求に応じてコンテンツを配信するが、その際に、上記のように選択した広告コンテンツを同時に配信する。また目的のコンテンツ自体をユーザの位置情報に応じて変更してもよい。

【００７５】コンテンツホルダ９０２は、オーディオ、ビデオ、あるいはテキストなどのコンテンツを取得もしくは製作する業者であり、コンテンツのバリューを設定し、該設定情報をコンテンツと共にコーディネータ９０１に提供し、配布されたコンテンツ量に応じてその対価を受け取る。

【００７６】広告クライアント９０３は、広告コンテンツの配布をコーディネータ９０１に依頼する広告提供者であり、広告コンテンツのバリューを設定し、該設定情報を広告コンテンツと共にコーディネータ９０１に提供し、配布された広告コンテンツ量に応じてその対価を支払う。

【００７７】また広告コンテンツにバリュー増加の属性を付加し、広告コンテンツを再生するとクーポンが貯まる、などの特典をつけることもできる。

【００７８】アクセスポイント９０４は、ネットワーク９０７への接続機能と、コンテンツ再生装置１１０との通信機能とを有し、コンテンツ再生装置１１０がネットワーク９０７に直接アクセスできない場合に、コンテンツ再生装置１１０がネットワーク９０７にアクセスするための中継装置となる。また、アクセスポイント９０４は、設置された地域の位置情報を記憶する手段と、該位置情報をコンテンツ配信サーバ１２０に送信する手段を有し、コンテンツ再生装置１１０とコンテンツ配信サーバ１２０間の通信が行われる際には、コンテンツ配信サーバ１２０に該位置情報を送信する。アクセスポイント９０４とコンテンツ配信サーバ１２０は、図９に示すように別個の装置することもできるし、一つの装置とすることもできる。アクセスポイント９０４とコンテンツ再生装置１１０との通信手段は、例えばbluetoothや携帯電話などの無線通信手段でもよいし、電話回線などの有線通信手段でもよい。また、コンテンツ配信サーバ１２０からコンテンツ再生装置１１０への情報伝達には地上波放送、衛星放送、ケーブルテレビなどの放送手段を使用し、コンテンツ再生装置１１０からコンテンツ配信サーバ１２０への情報伝達にはアクセスポイントを使用する、といった形態でもよい。

【００７９】キオスク端末９０５は、対価を受け取って課金装置１３０にバリュー値を補充する機能を持ち、例えば、駅やコンビニエンスストア、レコード店などに設置される。キオスク端末９０５はネットワーク９０７に接続する機能を有し、コーディネータ９０１はキオスク端末９０５を介して課金装置１３０とデータのやり取りをすることができる。ユーザがＩＣカードのような形態の課金装置１３０をコンテンツ再生装置１１０から取りはずし、その課金装置１３０をキオスク端末９０５に差込み、所定の操作をしてコーディネータ９０１のサーバに接続する、などの形態である。例えば、課金装置１３０にコンテンツ取得の履歴情報を記録しておき、コーディネータ９０１はキオスク端末９０５を介して該履歴情報を集計することで、市場の動向を推測したりする機能を設けることもできる。

【００８０】記憶装置９０６は、ネットワーク９０７に接続する機能を有する記憶装置であり、ユーザ毎に割り当てられた記憶領域を提供する機能を備え、コンテンツ再生装置１１０の外部記憶装置として利用できる。記憶装置９０６は、コンテンツ配信サーバ１２０や、コンテンツ再生装置１１０、課金装置１３０と安全に情報をやりとりするための暗号通信装置を備えていても良い。

【００８１】次に、図１１を用いて、図９に記載したアクセスポイントを利用して広告コンテンツを配信する手順について説明する。

【００８２】まず、コンテンツ再生装置１１０が、アクセスポイント９０４経由でコンテンツ配信サーバ１２０に接続する（ステップ１１０１，１１０２）。ここでコーディネータ９０１は、コンテンツ再生装置１１０がどのアクセスポイント９０４からアクセスしてきたのかを特定し、該アクセスポイント９０４の位置情報を取得する（ステップ１１０３）。次に該位置情報を利用して、コンテンツ再生装置１１０に送信する広告コンテンツを決定するが、この際、各広告コンテンツに定められた配布対象地域情報に基づいて、コンテンツ再生装置１１０の現在位置に適したコンテンツを選択する（ステップ１１０４）。最後に前記手段によって決定された広告コンテンツを図６に示した手順で暗号化し、コンテンツ再生装置１１０に送信する（ステップ１１０５～１１０７）。

【００８３】図１２は、コンテンツの取得時に課金をするシステムの一構成例である。ここで、記憶装置１２００および課金装置１３０は、それぞれデータを暗号化するための鍵を発行する手段と、該鍵で暗号化されたデータを復号化するための手段を持つ。ここで該鍵は、各装置毎にユニークな鍵を予め各装置が有していても良いし、乱数などによって毎回作成しても良い。ただし、該鍵は認証によって所有を許可された正当な装置以外には知られないようにする。記憶装置１２００は、例えば、コンテンツ再生装置１１０に内蔵されあるいは接続された記憶装置である。

【００８４】記憶装置１２００は、コンテンツ配信サーバ１２０に、コンテンツの配信要求と、記憶装置鍵Ksを送信する（１２０１）。次に、課金装置１３０が、コンテンツ配信サーバ１２０に課金装置鍵Kcを送信する（１２０２）。それを受けて、コンテンツ配信サーバ１２０は、要求されたコンテンツDを、記憶装置鍵Ksで暗号化し、さらに該暗号化コンテンツE(Ks,D)を課金装置鍵Kcで暗号化する。次にコンテンツ配信サーバ１２０は、該２重暗号化コンテンツE(Kc,E(Ks,D))を課金装置１３０に送信する（１２０３）。ここで、２重暗号化コンテンツE(Kc,E(Ks,D)))は、そのままではコンテンツ再生装置１１０で再生することはできないため、コンテンツを再生するには、課金装置１３０が必要になる。

【００８５】課金装置１３０は、受信した２重暗号化コンテンツE(Kc,E(Ks,D))を自身の保持する課金装置鍵Kcで復号し、その際の処理量に応じてバリュー値のカウンタVを変化させる（１２０４）。続いて、復号化されたコンテンツE(Ks,D)を記憶装置１２００に送信する（１２０５）。また、該課金装置１３０の保持するバリュー値Vが所定の範囲の値をとる場合、課金装置１３０は、２重暗号化コンテンツの復号を行うことができないようにする。

【００８６】該暗号化コンテンツを受信した記憶装置１２００は、自身の保持する記憶装置鍵Ksで該暗号化コンテンツE(Ks,D)を復号し、復号化された平文のコンテンツDを取得する（１２０６）。ここで、記憶装置１２００が受信した暗号化コンテンツE(Ks,D)は、該記憶装置鍵Ksを持つ記憶装置１２００以外では復号化することができないため、不正コピーを防ぐことができる。

【００８７】以上の処理において、記憶装置鍵Ksと課金装置鍵Kcは、それぞれの装置のもつ認証機能と暗号通信機能を利用して安全に送受される。

【００８８】記憶装置１２００からコンテンツ再生装置１１０へコンテンツを移動する際には、コンテンツ再生装置１１０がコンテンツ再生装置鍵を記憶装置に送信し、該鍵を使用して記憶装置１２００がコンテンツを暗号化し、コンテンツ再生装置１１０に送信する。

【００８９】図１３は、コンテンツの再生時に課金をするシステムの一構成例を示す図である。ここで、コンテンツ再生装置１１０および課金装置１３０は、それぞれデータを暗号化するための鍵を発行する手段と、該鍵で暗号化されたデータを復号化するための手段を持つ。ここで該鍵は、各装置毎にユニークな鍵を予め各装置が有していても良いし、乱数などによって毎回作成しても良い。ただし、該鍵は認証によって所有を許可された正当な装置以外には知られないようにする。

【００９０】コンテンツ再生装置１１０は、コンテンツ配信サーバ１２０にコンテンツの配信を要求し（１３０１）、課金装置１３０に課金装置鍵Kcの送信を要求する。それを受けて、課金装置１３０はコンテンツ配信サーバ１２０に課金装置鍵Kcを送信する（１３０２）。それを受けてコンテンツ配信サーバ１２０は、要求されたコンテンツDを課金装置鍵Kcを用いて暗号化し、記憶装置１３００に送信し（１３０３）、記憶装置１３００は受信した暗号化コンテンツE(Kc,D)を格納する（１３０４）。

【００９１】次に、コンテンツ再生装置１１０は、コンテンツ再生装置鍵Kpを課金装置１３０に送信する（１３０５）。つづいて、記憶装置１３００は該暗号化コンテンツE(Kc,D)を課金装置１３０に送信する（１３０６）。課金装置１３０は、受信した暗号化コンテンツE(Kc,D)を課金装置鍵Kcで復号し、そのコンテンツDの属性に応じてバリュー値カウンタVを変化させる（１３０７）。次に復号化されたコンテンツDを今度はコンテンツ再生装置鍵Kpで暗号化し、コンテンツ再生装置１１０に送信する（１３０８）。コンテンツ再生装置１１０は、該暗号化コンテンツE(Kp,D)をコンテンツ再生装置鍵Kpを用いて復号化し、コンテンツDを再生する（１３０９）。

【００９２】ここで、暗号化コンテンツE(Kc,D)は課金装置鍵Kcを使用しないと復号化することができないため、安全に記憶装置１３００上に保管することができる。またコピーも自由である。このため、コンテンツ配信サーバ１２０から記憶装置１３００へ暗号化コンテンツE(Kc,D)を送信するセッション（１３０１～１３０４）と、該コンテンツE(Kc,D)をコンテンツ再生装置１１０に送信するセッション（１３０５～１３０９）とは、分離することができる。

【００９３】また、該記憶装置１３００は、コンテンツ再生装置１１０や課金装置１３０に内蔵されていても良いし、ネットワーク上に接続されている記憶装置でも良い。その場合、コンテンツ再生装置１１０または課金装置１３０は、例えばネットワークアドレスなどを記憶する機能を有し、該記憶装置１３００へのアクセス手段を有するものとする。こうすることで、コンテンツ再生装置１１０は大容量の記憶装置を内蔵する必要がなくなり、また、複数のコンテンツ再生装置１１０を有している場合も、コンテンツデータの共有を容易に行うことができる。

【００９４】以上の処理において、コンテンツ再生装置鍵と課金装置鍵は、それぞれの装置の持つ認証機能と暗号通信機能を利用して安全に送受される。

【００９５】以上、本発明の一実施形態について説明をした。なお、本発明は、前記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【００９６】

【発明の効果】以上説明したように、本発明によれば、コンテンツ著作権を保護する機能と、コンテンツの使用に対して、その使用量に応じて従量制で適宜課金する機能を備えたコンテンツ配信を行うことが可能になる。またコンテンツを視聴するとユーザが特典を得ることのできるコンテンツや、ユーザの位置情報に応じた好適なコンテンツを配信することができる。

【図面の簡単な説明】

【図１】本発明の概念を示す図。

【図２】課金装置の概略構成を示す図。

【図３】コンテンツ再生装置の概略構成を示す図。

【図４】オーディオ再生装置の概略構成を示す図。

【図５】ビデオ再生装置の概略構成を示す図。

【図６】コンテンツ配信システムのコンテンツ配信手順を示す図。

【図７】コンテンツ配信手順を示すフロー図。

【図８】コンテンツ配信サーバ、コンテンツ再生装置、および課金装置間のデータのやり取りの一例を説明するためのシーケンス図。

【図９】コンテンツ配信システムの概観を示す図。

【図１０】コンテンツの属性情報の概念を示す図。

【図１１】コンテンツ配信システムにおける広告コンテンツの配信手順を示すフロー図。

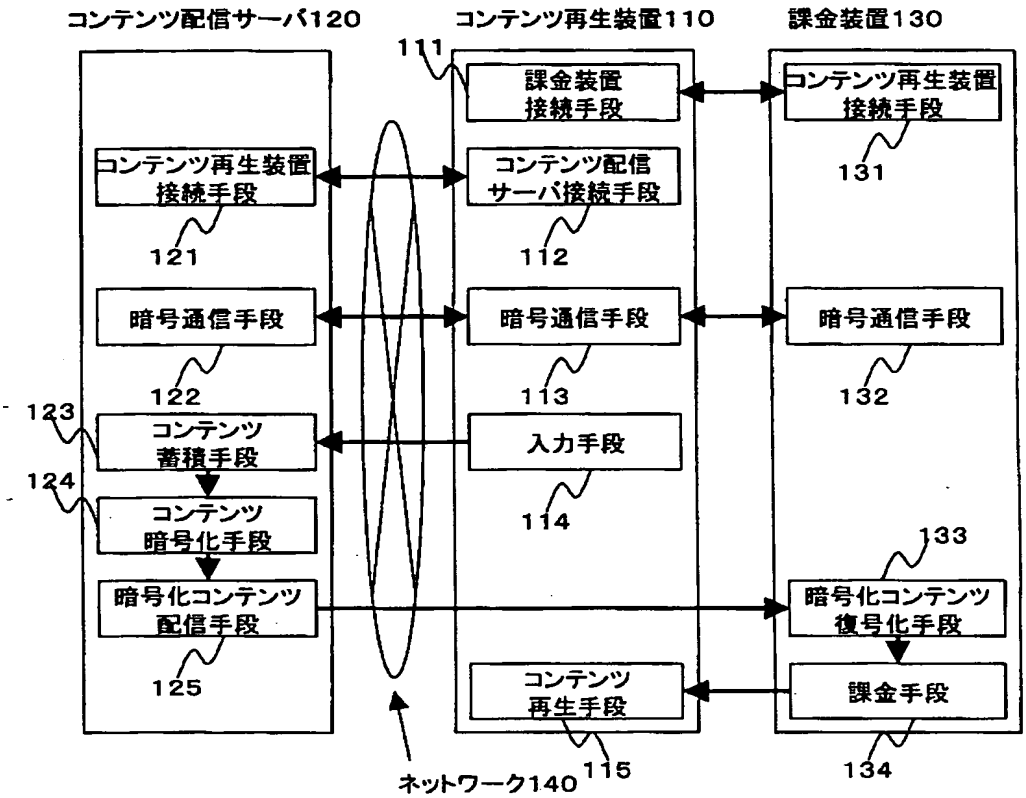
【図１２】コンテンツ配信システムのコンテンツ配信手順を示す図。

【図１３】コンテンツ配信システムのコンテンツ配信手順を示す図。

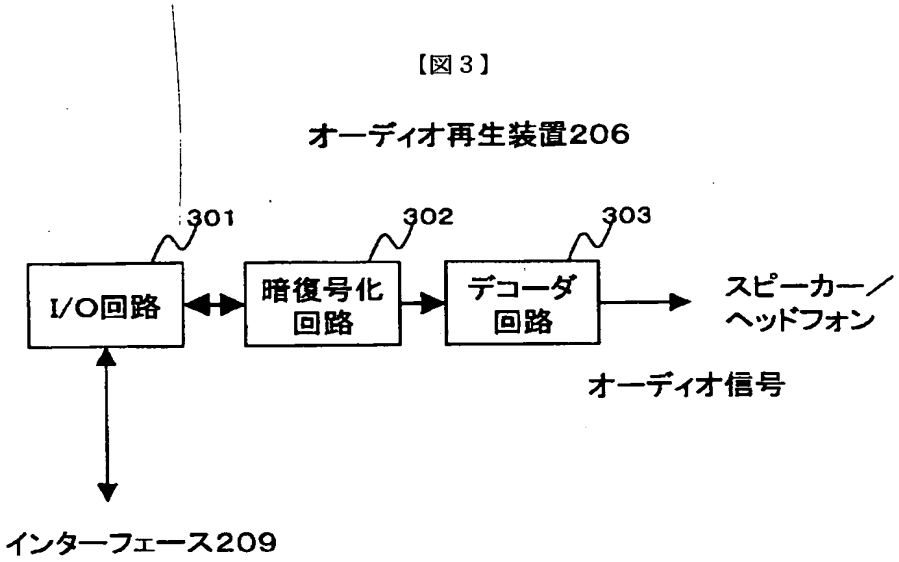
【符号の説明】

１１０…コンテンツ再生装置
１１１…課金装置接続手段
１１２…コンテンツ配信サーバ接続手段
１１３、１２２、１３２…暗号通信手段
１１４…入力手段
１１５…コンテンツ再生手段
１２０…コンテンツ配信サーバ
１２１…コンテンツ再生装置接続手段
１２３…コンテンツ蓄積手段
１２４…コンテンツ暗号化手段
１２５…暗号化コンテンツ配信手段
１３０…課金装置
１３１…コンテンツ再生装置接続手段
１３３…暗号化コンテンツ復号化手段
１３４…課金手段
２０１…ＣＰＵ
２０２…メモリ
２０３…入力装置
２０４…通信装置
２０５…課金装置接続装置
２０６…オーディオ再生装置
２０７…ビデオ再生装置
２０８…表示装置
３０１、４０１、５０４…Ｉ／Ｏ回路
３０２、４０２、５０１…暗復号化回路
３０３、４０３…デコーダ回路
５０２…課金回路
５０３…バリュー値カウンタ
５０５…記憶回路
５０６…タンパレジスタント領域
９０１…コーディネータ
９０２…コンテンツホルダ
９０３…広告コンテンツ
９０４…アクセスポイント
９０５…キオスク端末
９０６、１２００、１３００…記憶装置
９０７…ネットワーク
９０８…通信手段

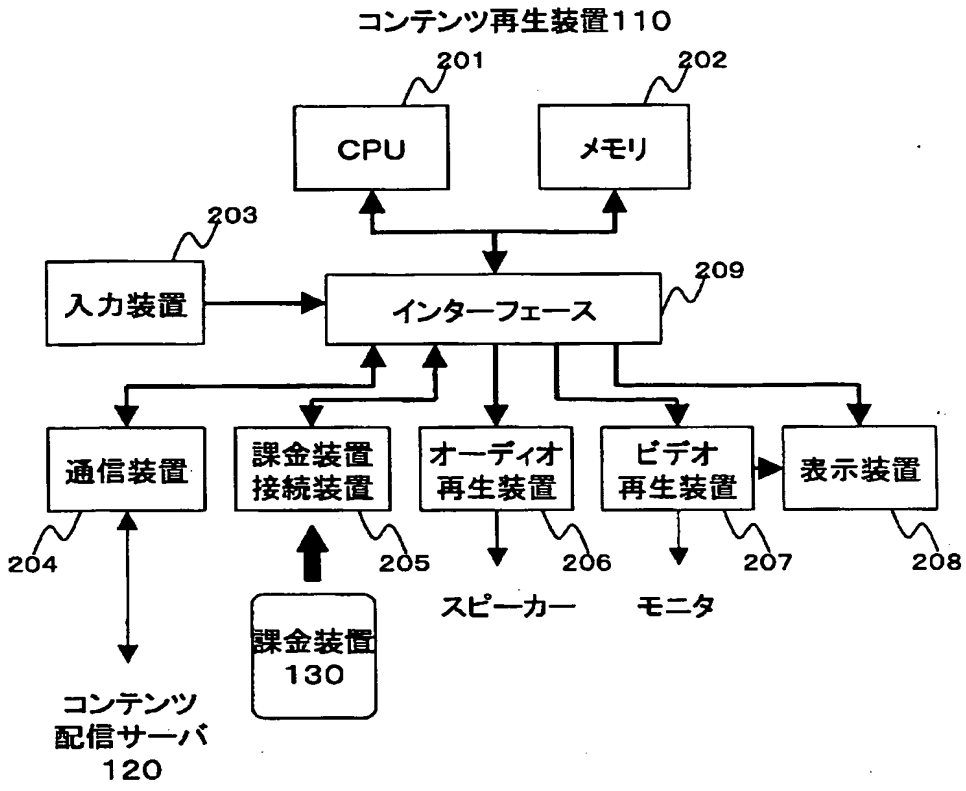
【図１】


コンテンツ配信サーバ120
コンテンツ再生装置110
課金装置130
111
課金装置接続手段
コンテンツ再生装置接続手段
131
コンテンツ再生装置接続手段
121
コンテンツ配信サーバ接続手段
112
暗号通信手段
暗号通信手段
暗号通信手段
122
113
132
123
コンテンツ蓄積手段
入力手段
124
114
コンテンツ暗号化手段
133
暗号化コンテンツ配信手段
暗号化コンテンツ復号化手段
125
コンテンツ再生手段
課金手段
115
134
ネットワーク140

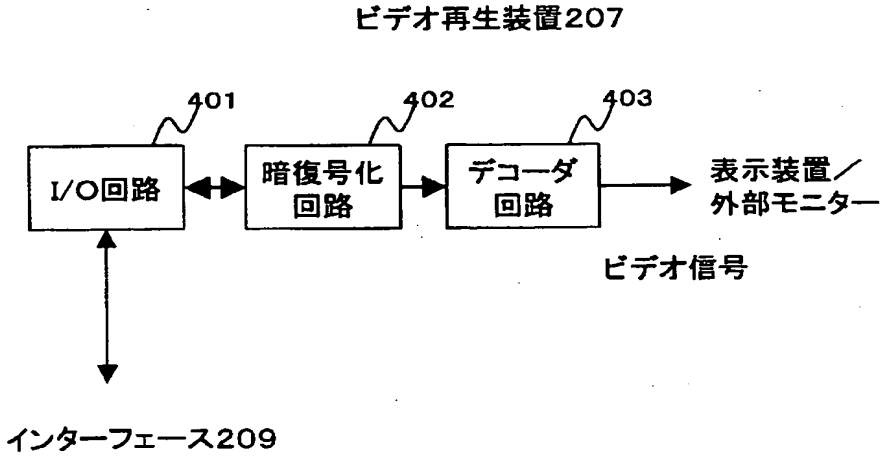
【図３】


オーディオ再生装置206
301
302
303
I/O回路
暗復号化回路
デコーダ回路
スピーカー／ヘッドフォン
オーディオ信号
インターフェース209

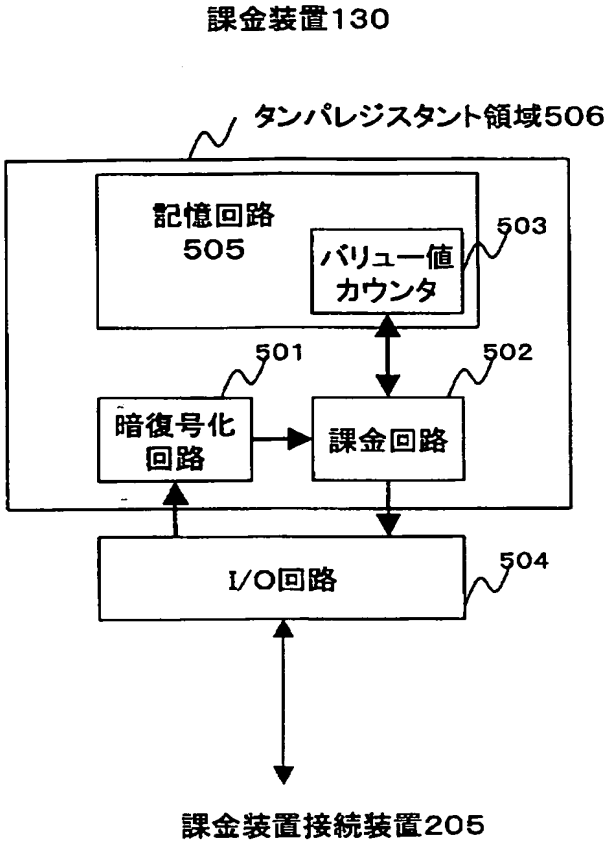
【図２】


コンテンツ再生装置110
201
202
CPU
メモリ
203
入力装置
209
インターフェース
通信装置
課金装置
接続装置
オーディオ
再生装置
ビデオ
再生装置
表示装置
204
205
206
207
208
スピーカー
モニタ
課金装置
130
コンテンツ
配信サーバ
120

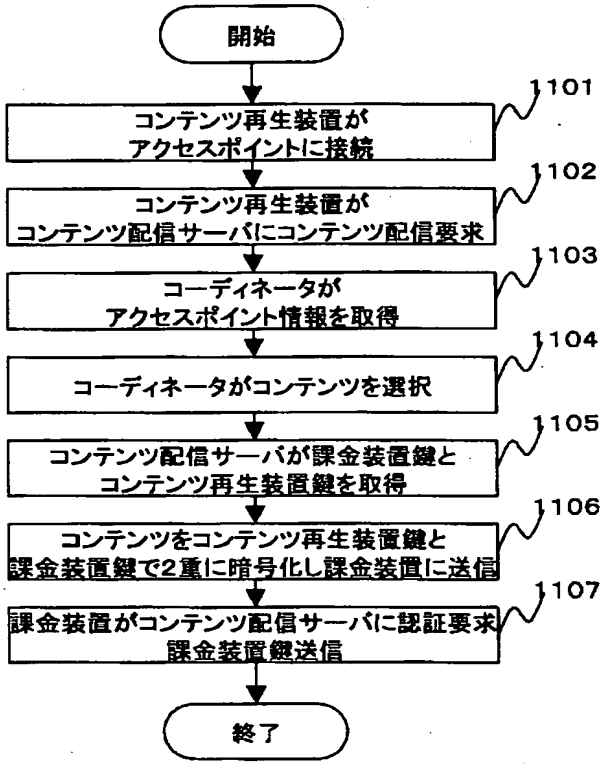
【図４】


ビデオ再生装置207
401
402
403
I/O回路
暗復号化
回路
デコーダ
回路
表示装置／
外部モニター
ビデオ信号
インターフェース209

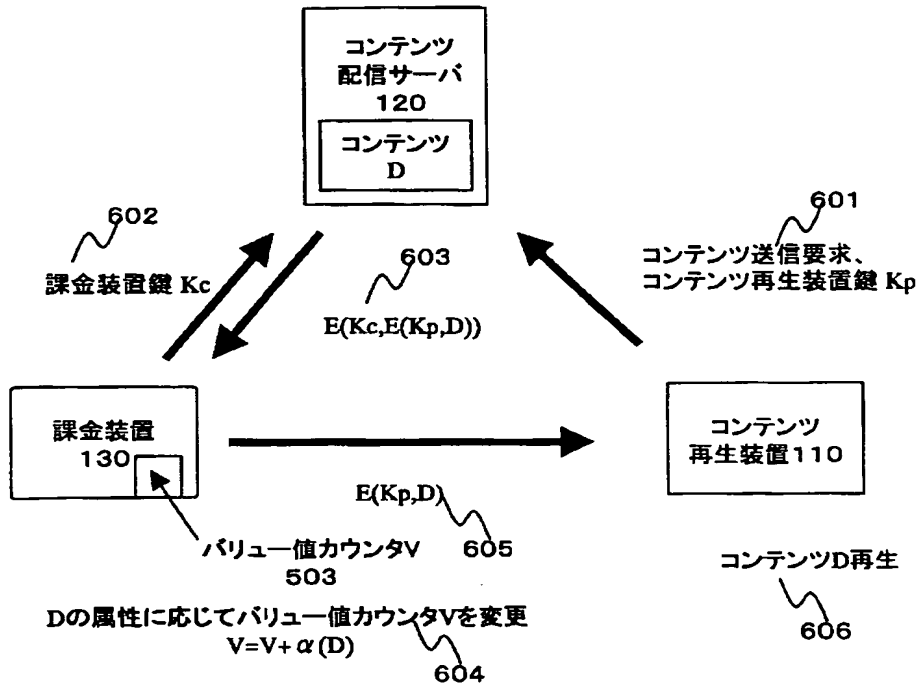
【図５】


課金装置130
タンパレジスタント領域506
記憶回路
505
バリュー値
カウンタ
503
501
502
暗復号化
回路
課金回路
I/O回路
504
課金装置接続装置205

【図１１】

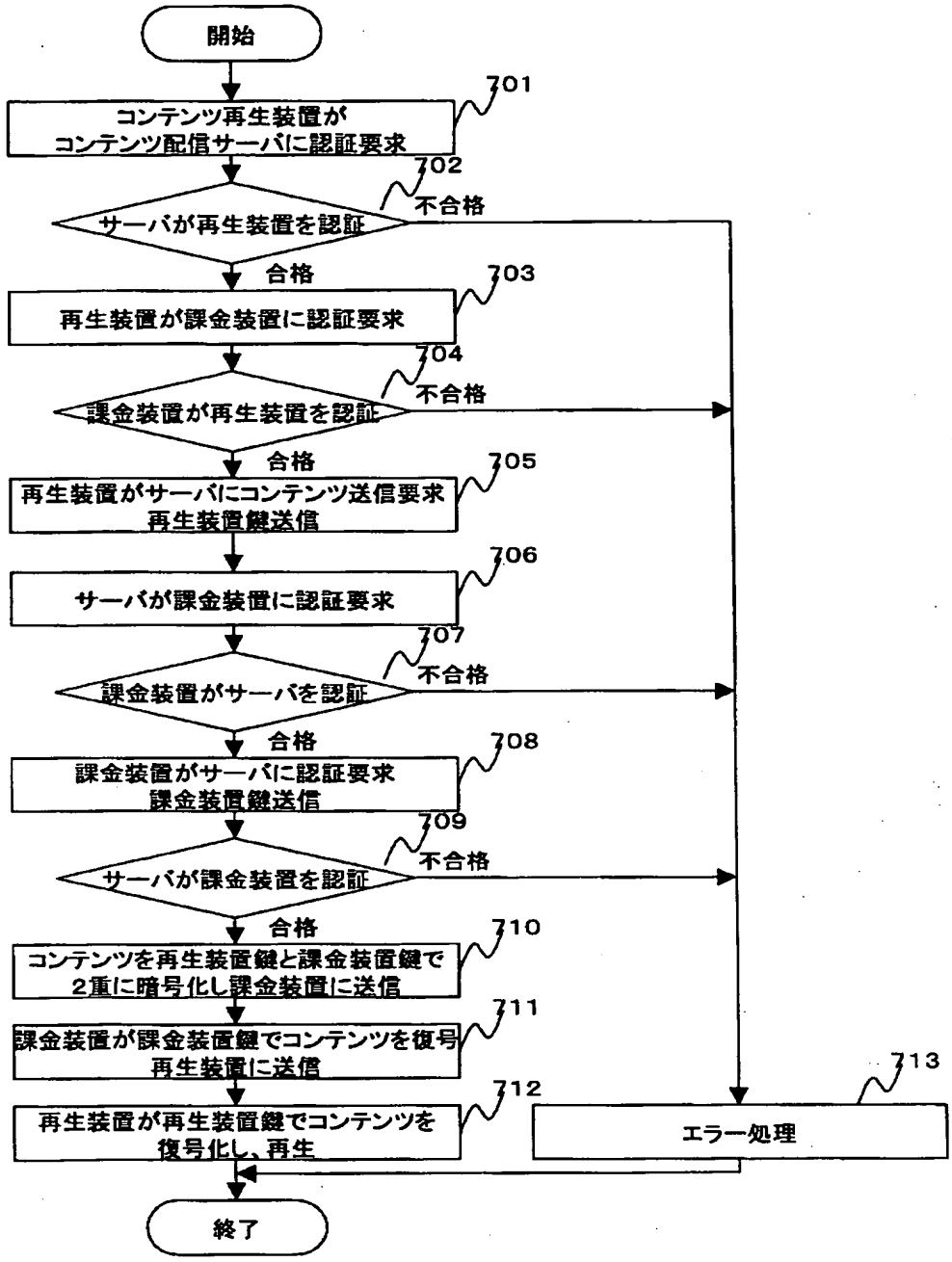

開始
コンテンツ再生装置が
アクセスポイントに接続
1101
コンテンツ再生装置が
コンテンツ配信サーバにコンテンツ配信要求
1102
コーディネータが
アクセスポイント情報を取得
1103
コーディネータがコンテンツを選択
1104
コンテンツ配信サーバが課金装置鍵と
コンテンツ再生装置鍵を取得
1105
コンテンツをコンテンツ再生装置鍵と
課金装置鍵で2重に暗号化し課金装置に送信
1106
課金装置がコンテンツ配信サーバに認証要求
課金装置鍵送信
1107
終了

【図６】

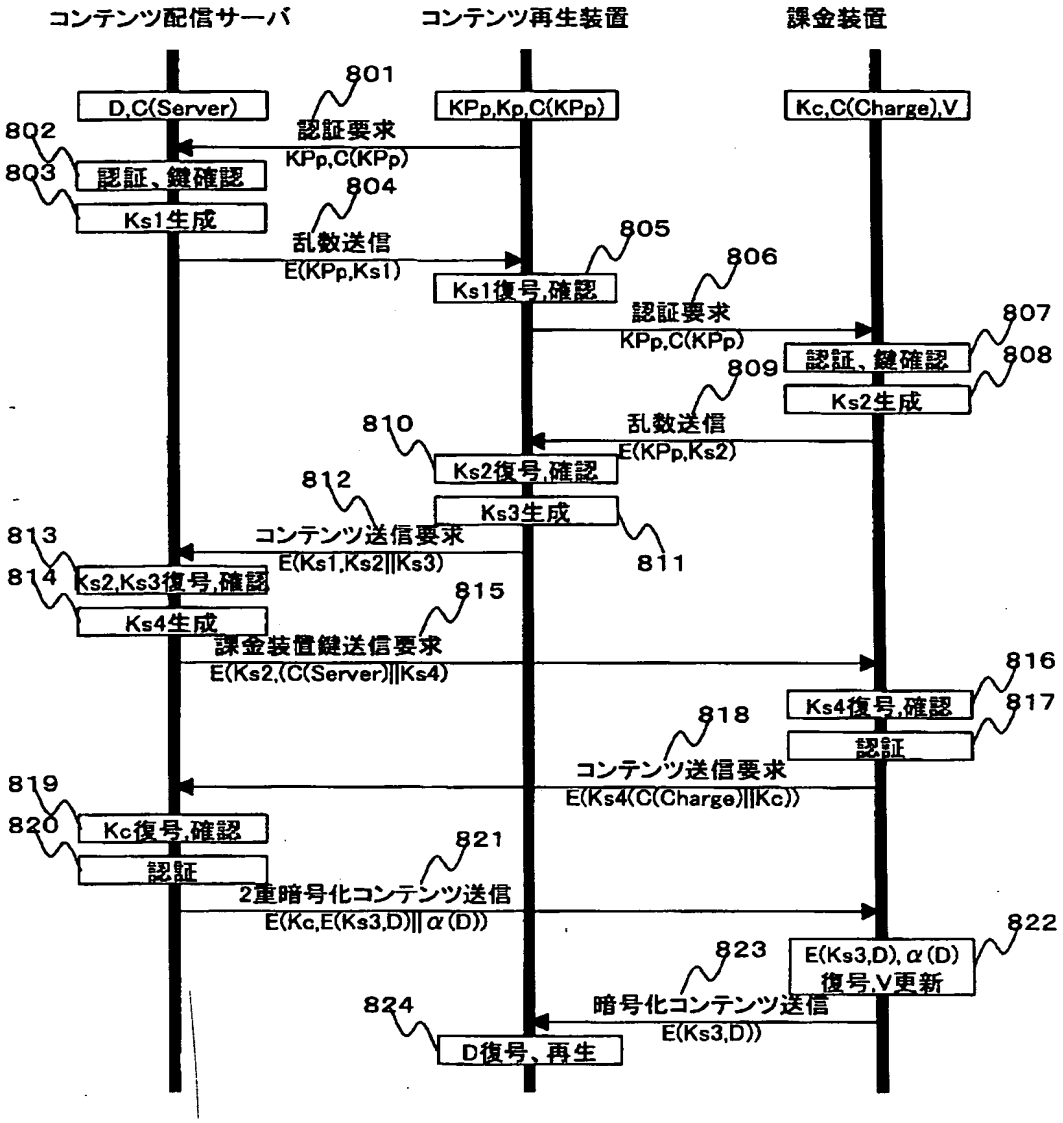


E(xx,yy)：鍵xxでyyを暗号化したデータ
α(zz)　：データzzに定められたVの変化量

【図７】


開始
701
コンテンツ再生装置が
コンテンツ配信サーバに認証要求
702
サーバが再生装置を認証
不合格
合格
703
再生装置が課金装置に認証要求
704
課金装置が再生装置を認証
不合格
合格
705
再生装置がサーバにコンテンツ送信要求
再生装置鍵送信
706
サーバが課金装置に認証要求
707
課金装置がサーバを認証
不合格
合格
708
課金装置がサーバに認証要求
課金装置鍵送信
709
サーバが課金装置を認証
不合格
合格
710
コンテンツを再生装置鍵と課金装置鍵で
2重に暗号化し課金装置に送信
711
課金装置が課金装置鍵でコンテンツを復号
再生装置に送信
712
再生装置が再生装置鍵でコンテンツを
復号化し、再生
713
エラー処理
終了

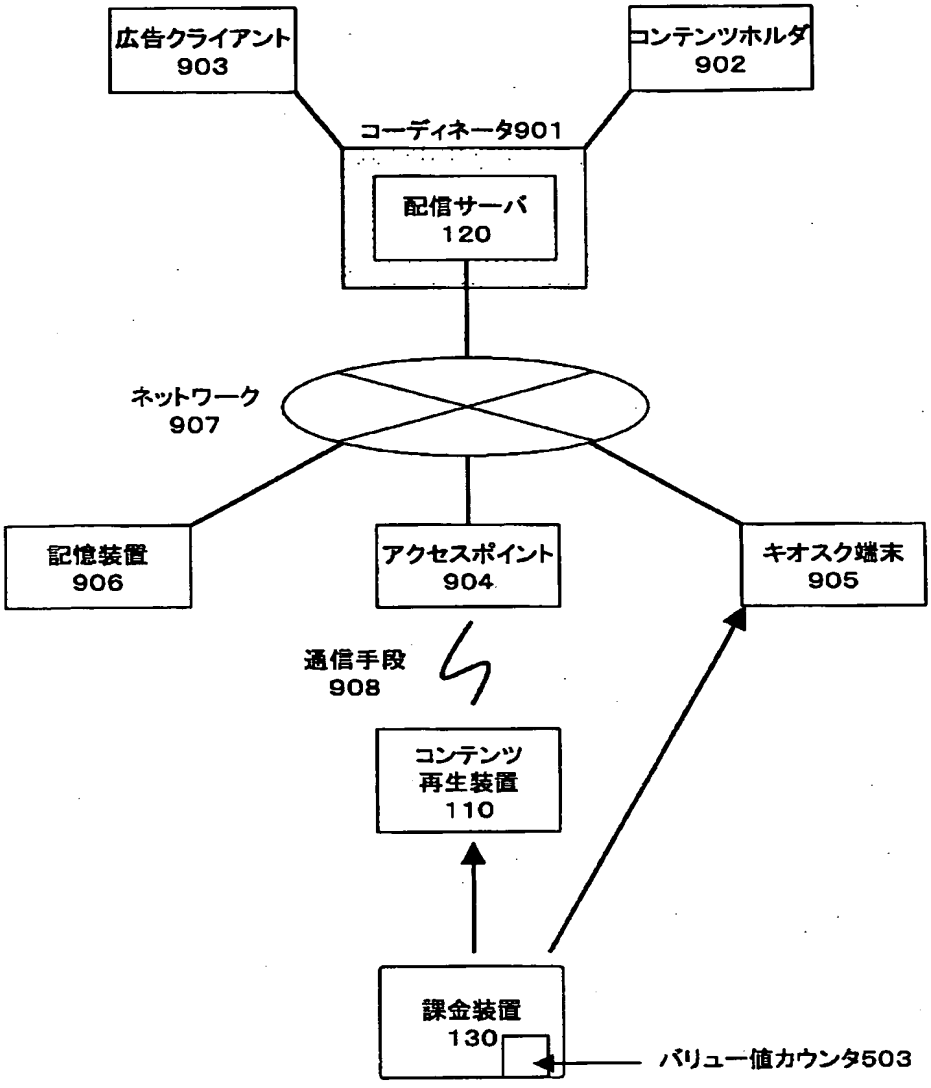
【図８】



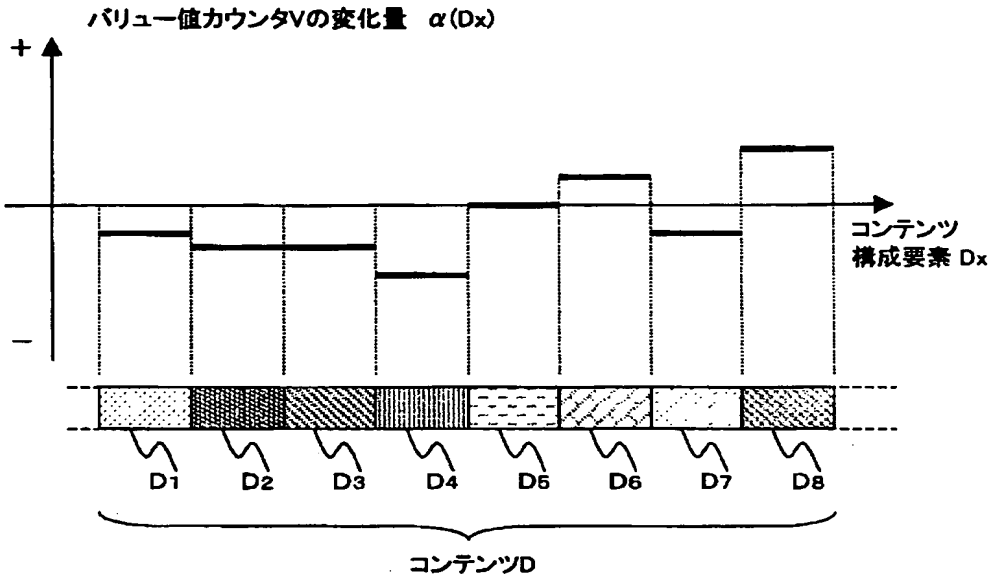
D:コンテンツデータ
V:バリュー値
C(ww):wwの証明書
E(xx,yy):鍵xxでyyを暗号化したデータ
α(zz):データzzに定められたVの変化量

KPp:コンテンツ再生装置公開鍵
Kp:コンテンツ再生装置秘密鍵
Kc:課金装置鍵
Ksx:セッション鍵

【図９】

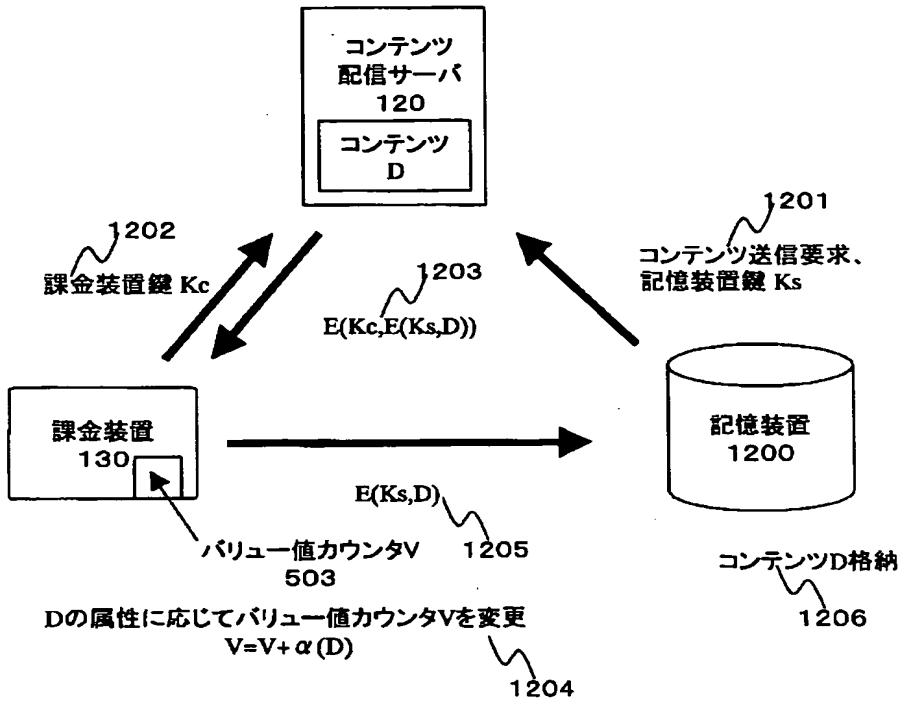

広告クライアント
903
コンテンツホルダ
902
コーディネータ901
配信サーバ
120
ネットワーク
907
記憶装置
906
アクセスポイント
904
キオスク端末
905
通信手段
908
コンテンツ
再生装置
110
課金装置
130
バリュー値カウンタ503

【図１０】



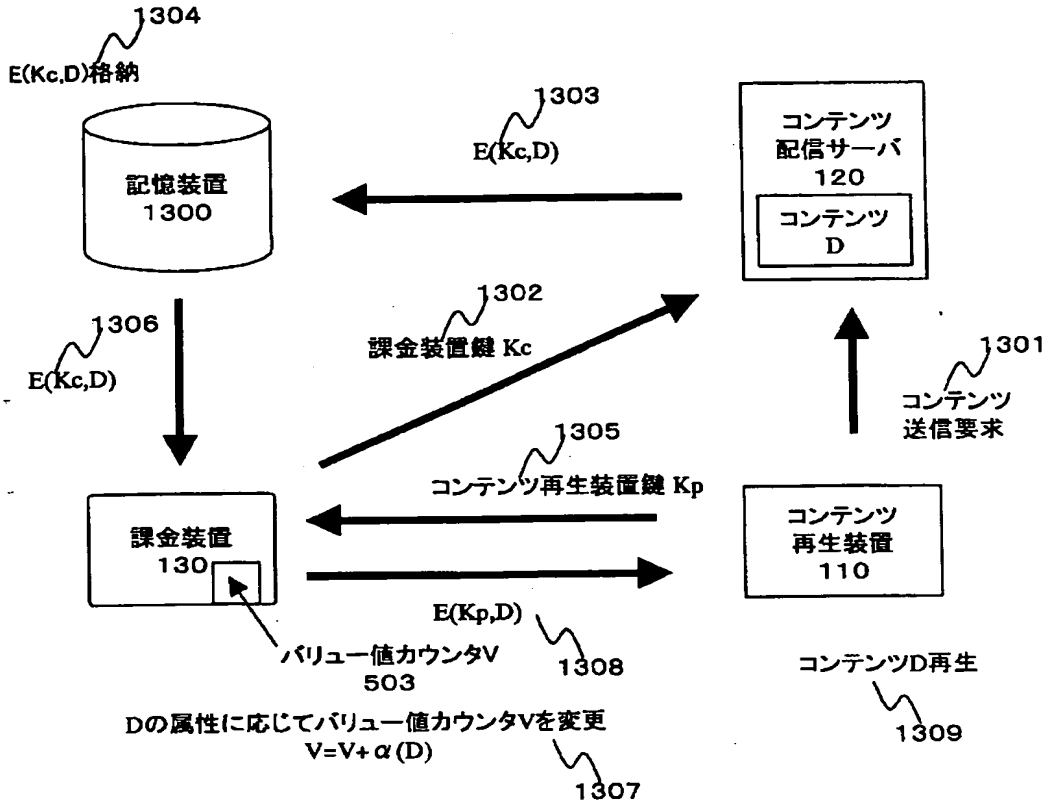
α(xx)　：データxxに定められたVの変化量

【図１２】



E(xx,yy)：鍵xxでyyを暗号化したデータ
α(zz)　：データzzに定められたVの変化量

【図１３】



E(xx,yy):鍵xxでyyを暗号化したデータ
α(zz) :データzzに定められたVの変化量

フロントページの続き

(51)Int.Cl.[7]		識別記号	FI		テーマコード（参考）
Ｈ０４Ｌ	9/32		Ｈ０４Ｎ	7/16	Ｃ
Ｈ０４Ｎ	7/16			7/173	６１０Ｚ
	7/173	６１０			６４０Ａ
		６４０	Ｈ０４Ｌ	9/00	６７３Ａ

(72)発明者　常広　隆司
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　角田　元泰
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　井口　慎也
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　水島　永雅
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

Ｆターム(参考)　5C064 BA07 BB01 BB10 BC01 BC17
BC18 BC22 BC23 BD02 BD04
BD08 BD09 CA14 CB06 CC04
5J104 AA01 AA07 AA16 EA06 EA17
KA01 NA02 PA07 PA11